УДК 007.4 **Юридические науки**

Фаргиева Зульфия Султангиреевна, *преподаватель физико — математический факультет кафедра математики и ивт, Ингушский государственный университет г. Магас*

Катиева Лиза Магомедовна, *студентка 3 курса физико — математический факультет специиальность -информационные системы и технологии кафедра математики и ивт, Ингушский государственный университет г. Магас*

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ В БАНКОВСКОЙ СФЕРЕ: ПРОФИЛАКТИКА, ПРЕДУПРЕЖДЕНИЕ

Аннотация: в статье описана проблема кибермошенничества в банковской сфере, отражены способы выявления и противодействия данным преступлениям. Цель исследования – доказать актуальность угрозы киберпреступности для кредитно-финансовой сферы, сама актуальность состоит в огромных объемах хищений, а также в постоянной разработке хакерами принципиально новых способов кражи. Для анализа текущей ситуации были использованы данные исследований организаций, занимающихся компьютерной безопасностью, а также данные МВД России. В результате исследования были обобщены основные методы выявления и противодействия киберпреступлениям, обоснована актуальность выбранной проблемы.

Ключевые слова: киберпреступность, информационные технологии, кибермошенничество, хакеры, вирусы, банк, интернет, киберпреступники, киберпространство.

Abstract: the article describes the problem of cybercrime in the banking sector, reflects the ways to identify and counteract these crimes. The purpose of the study is to prove the relevance of the cybercrime threats to credit and financial sphere, the relevance is huge amounts of theft, and the ongoing development of hackers of new

methods of theft. To analyze the current situation, we used research data from organizations involved in computer security, as well as data from the Ministry of internal Affairs of Russia. The text shows the types of cybercrime, as well as a scheme for identifying criminal persons responsible for organizing the crime. Because of the research, the main methods of detecting and countering cybercrime were summarized, and the relevance of the chosen problem was substantiated.

Key words: cybercrime, information technology, cyber fraud, hackers, viruses, Bank, Internet, cybercriminals, cyberspace.

Киберпреступление, как и другие виды преступлений, является работой одного или нескольких злоумышленников, в данном случае с колоссальными знаниями в области интернета и цифровых технологий, которые используют для достижения корыстных целей [1]. Наиболее привлекательна для преступников банковская сфера, ведь она осуществляет ежедневно огромное количество транзакций и осуществляет оборот огромного количества денежных средств. В условиях постоянного развития информационных технологий у мошенников появляются все новые и новые способы достижения своих преступных целей. В связи с этим с каждым годом увеличивается количество атак, а следовательно, появляется необходимость своевременного реагирования, предупреждения и предотвращения мошеннических действий.

Организациям важно постоянно обновлять свою систему безопасности, обеспечивать постоянный мониторинг ситуации и сотрудничать с компаниями, занимающимися разработкой и улучшением программного обеспечения, которое защищает электронные устройства от посягательств киберпреступников. Не менее важно, как данные преступления трактует государство и какое наказание понесут преступники.

Расширение глобальной сети Интернет требовало применения все более наукоемких технологий для обеспечения ее (сети) бесперебойной работы, что делало данную площадку все более удобной и привлекательной для пользователей. Вследствие развития информационных технологий практически

все виды финансовых организаций стали не только предоставлять свои услуги в киберпространстве, но также начали производить практически все свои операции через электронные системы. Киберпространство (англ. cyberspace) – метафорическая абстракция, используемая в философии и в компьютерных технологиях, является виртуальной реальностью, которая представляет ноосферу. Ноосфера – сфера взаимодействия общества и природы, в границах которой разумная человеческая деятельность становится определяющим фактором развития.

Преступления в сети относительно новая, но быстро развивающаяся сфера деятельности для злоумышленников. Отдельное внимание устремлено на социальные сети и мобильные устройства, в этой области пользователи наименее информированы о киберугрозах. Хакерские атаки становятся более сложнее и профессиональнее, они направляются не только на индивидуальных пользователей, но и на промышленные системы. Как показало исследование компании Juniper Research, при сохранении текущего уровня кибератак общие убытки мировой экономики от их осуществления составили 2,1 триллиона долл. до 2019 г.

Киберпреступность – это следствие глобализации информационно-коммуникационных технологий и появления международных компьютерных сетей.

Анализируя ситуацию непосредственно в России, наблюдаем в основном преступления в финансовой сфере. С целью кражи денежных средств их совершают хакерские группы Cobalt, MoneyTaker, Lazarus, часть из которых русскоязычные. Приведенные группировки на сегодняшний день являются самыми опасными для банков на международной арене, им не составит огромного труда атаковать и вывести из строя банк, а позже изъять денежные активы. В 2018-ом году была выявлена новая хакерская группировка – Silence, которую нарекли «новой угрозой для банков».

Известно, что в нашей стране количество киберпреступлений растет из года в год, так как эта сфера преступлений пока еще остается проблематичной для ее предупреждения и оперативной борьбы с ней.

Стоит отметить, что организации, специализирующиеся на разработке защиты от посягательств киберпреступников, постоянно создают и улучшают свои защитные системы, которые предлагают для установки в финансовые организации. Но основная проблема заключается во времени обнаружения и в способности оперативно устранять угрозы, а также вычислять преступников.

По данным международной компании Group-IB, которая занимается расследованием и предотвращением киберпреступлений, в среднем в России каждый месяц успешно взламывают 1–2 банка: средний ущерб такого киберограбления составляет 132 млн рублей (примерно, 2 млн долларов) [1].

Объем хищений денежных средств у юридических лиц, а также у банковских организаций с помощью вредоносных программ для ПК, ежегодно продолжит снижаться на российском рынке, так как большинство профессиональных хакерских групп переориентировались на страны с более слабой информационной безопасностью, да и в целом основной целью киберпреступников станут физические лица, как наиболее слабое звено финансовой системы.

Из-за динамично развивающихся информационных технологий виды финансовых кибератак видоизменяются, а схемы получения противозаконного заработка с каждым годом становятся все изощреннее. На данный момент можно выделить следующие виды финансово ориентированных киберпреступлений [2]:

- фишинг – это один из видов интернет-мошенничества, целью которого является получение доступа к средствам аутентификации клиента, к конфиденциальным данным пользователей – паролям и логинам учетной записи в системе электронного банкинга;
- программы-вымогатели – программы, ограничивающие доступ пользователя к электронному устройству и требующие выкуп за возвращения права доступа;

- финансовое мошенничество – это вид преступных действий, которые осуществляются с помощью информационных систем и направлены на кражу у пользователей конфиденциальных данных и финансовых средств;

- шпионская программа – тип вредоносного программного обеспечения, присутствие которого в системе является практически незаметным для пользователей и частично невозможным к обнаружению;

- ботнет (сеть ботов) – это компьютерная сеть, на устройства которой скрытно установлено вредоносное ПО, позволяющее киберпреступникам удаленно управлять вычислительными ресурсами зараженных устройств.

Сотни или даже тысячи зараженных таким программным обеспечением устройств используются злоумышленниками для рассылки спама и вирусов, кражи личных данных пользователей и DDoS атак. На сегодняшний день данная угроза является одной из самых серьезных среди киберугроз.

Большинство атак нужно предотвращать еще на этапе их подготовки при помощи новейших программ.

Внутри организаций применяются следующие этапы алгоритма выявления кибермошенничества [3]:

- возникновение факта киберпреступления у кредитной организации (банка);

- проведение проверки сотрудниками кредитной организации либо лабораториями МВД, либо наемной компании, специализирующейся на киберпреступлениях;

- проведение допроса штата сотрудников кредитной организации, где отмечаются странности в поведении или пренебрежение должностными полномочиями и инструкциями;

- срочно опечатывается и изымается компьютер, который непосредственно имеет отношение к хищению денежных средств;

- в ходе исследования эксперты выявляют псевдоним преступника, его IP-адрес, была ли это преступная группировка и кто же все-таки управлял операциями по хищению денег;

- обращение в правоохранительные органы с информацией о совершении преступления;

- предоставление заявления и отчетных материалов служебной проверки по поводу хищения денежных средств от кредитной организации, а также экспертное заключение от специалистов по киберпреступлениям.

Важно понимать, как можно выявить и предотвратить киберпреступления. Основными способами противодействия угрозам являются постоянный мониторинг и своевременное обновление защитных систем.

К сожалению, атаки чаще всего замечают спустя короткое время после их начала, но к этому времени злоумышленники уже успевают украсть достаточно большую сумму денег. Атаки на банковские организации готовятся и планируются преступниками долгое время – доходит даже до одного года. Следовательно, попытки хакеров взломать систему безопасности организаций нужно стараться идентифицировать на самом раннем этапе подготовки кибератаки, чтобы избежать убытков как таковых [5].

Огромную роль в противодействии киберпреступникам играет обратная связь кредитно-финансовых организаций с организациями, специализирующимися на обнаружении и устранении киберугроз, а также с государственными органами, которые будут выявлять и привлекать преступников к ответственности.

Правильным утверждением является невозможность противодействия экономическим преступлениям, в частности кибермошенничеству, без взаимодействия государств и международных организаций, которые осуществляют помощь в предупреждении и борьбе с киберугрозами. Чтобы эффективно противостоять киберпреступникам, в государстве необходимо выстроить многоуровневую систему кибербезопасности, которая смогла бы защищать и интересы простых граждан, и государственные или частные организации [3].

Ситуация по киберпреступлениям в России двоякая: с одной стороны, наблюдается увеличение количества преступлений с использованием

информационных технологий; с другой – снижается объем хищений в финансовой сфере. В данный момент киберпреступления опасны тем, что преступники осуществляют свои действия дистанционно, а также способны за короткий срок с момента начала преступления украсть огромные суммы денег. Разработчики антивирусных программ постоянно обновляют свои защитные системы, а также изучают и нейтрализуют возникающие опасности [4].

Библиографический список:

1. «Компания Avast о типах киберугроз» [Электронный ресурс]. – Режим доступа: https://www.avast.ru/c-malware (дата обращения: 23.08.2020).
2. Белякова И. М., Добрина Т. Б. // Эпоха науки, 2018. – №14. – url: https://cyberleninka.ru/article/n/problema-rassledovaniya-ekonomicheskih-prestupleniy-sovershennyh-s-ispolzovaniem-informatsionnyh-tehnologiy-i-setevogo-prostranstva.
3. Головинов О.Н., Погорелов А.В. (2016). Киберпреступность в современной экономике: состояние и тенденции развития. Вопросы инновационной экономики, №6(1), 73-88. [Электронный ресурс]. – Режим доступа: doi:10.18334/vinec.6.1.35353 (дата обращения: 23.08.2020).
4. Отчет о тенденциях высокотехнологичных преступлений 2018 [Электронный ресурс]. – Режим доступа: https://www.group-ib.ru/resources/threat-research/2018-report.html (дата обращения: 23.08.2020).
5. Тарасов А Электронный банкинг и его безопасность// Экономическая политика, 2010. – №5. – url: http://ecsocman.hse.ru/data/2012/12/18/1251395379/9.pdf.